



## Small Business IT Risk Assessment

Company name:			
Completed by:		Date:	

### Where Do I Begin?

A risk assessment is an important step in protecting your customers, employees, and your business, as well as complying with the law. This Information Technology Risk Assessment survey helps identify all of the information assets you handle, the controls in place, and areas of high risk or threats. Steps for completing this risk assessment:

- Step 1: Complete the questionnaire below. Use additional paper as needed to add notes or new survey questions.
- Step 2: Based on your responses apply a risk rating for each of the applicable categories.  
Rate your risk on a scale of 1-5, with 1 being the least secure, and 5 the most secure.
- Step 3: List specific areas of high risk or threats, along with any new control that may be needed
- Step 4: Present your findings to management and the board, and implement new controls as needed.
- Step 5: Update your risk assessment at least once a year, comparing your results to previous versions

I. Company Information			
Business primary address:			
Phone:		Date company was formed:	
Number of employees (FTE):			
Type of business (check one):	<input type="checkbox"/> Corporation <input type="checkbox"/> Partnership <input type="checkbox"/> Individual <input type="checkbox"/> Other _____		
Nature of business:			
Website url(s):			
Do you conduct business outside the US?	<input type="checkbox"/> Yes <input type="checkbox"/> No	If yes, identify countries:	

II. Management Supervision	
<i>Management and board supervision are essential for an effective information security program, and often mandated by state and federal regulations.</i>	
Do you have a written information security plan?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are you aware of, and in compliance with, any laws mandating information security?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are adequate data protection procedures in place and monitored by management?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do you use third party vendors for managing your network?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do third party vendor contracts provide adequate controls?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are third party contracts monitored at least annually?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are sufficient procedures in place for incident reporting?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do you have a business continuity plan and/or disaster recovery plan?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do you deliver up-to-date security training to management and staff?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

Is the Board actively involved with your information security plans and procedures?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
---	---

Rate your Management Supervision risk on a scale of 1-5, with 1 being the least secure, and 5 the most secure:	
Least Secure	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 Most Secure
Reason for the rating:	
List areas of high risk (threats):	List new controls needed:

III. Personnel Security	
<i>Pre-employment screening, such as background checks, should be conducted for individuals that will handle sensitive information.</i>	
Do you perform background checks on all employees with access to sensitive information?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do background checks include criminal history?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are photo IDs required for employment?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are photo IDs or visitor badges worn in the workplace?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do you delete security access immediately upon employee termination?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

Rate your Personnel Security risk on a scale of 1-5, with 1 being the least secure, and 5 the most secure:	
Least Secure	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 Most Secure
Reason for the rating:	
List areas of high risk (threats):	List new controls needed:

#### IV. Physical Security

*This section helps identify the physical security controls in place, and determine if any physical weaknesses exist for protecting sensitive information*

Is access to the building(s) securely maintained during business hours and after hours?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are sufficient locks maintained on all doors, windows, and entrances?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do you have a security alarm system?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do you have security cameras on premise?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are employees and/or visitors required to wear badges?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Is the building(s) adequately protected against fire?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Does the building(s) have a fire alarm system?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Is the building(s) protected with sprinklers?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are sensitive files and documents stored in fireproof files or vaults?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Is the building(s) adequately protected against water damage?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Is access to network equipment such as servers and storage media containing sensitive data physically protected? (Check all that apply)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
<input type="checkbox"/> Areas are restricted to authorized employees only	<input type="checkbox"/> Software permission controls
List other physical security issues for your business:	

**Rate your Physical Security risk on a scale of 1-5, with 1 being the least secure, and 5 the most secure:**

Least Secure	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5	Most Secure
Reason for the rating:		
List areas of high risk (threats):		List new controls needed:

## V. Identify Your Information Assets

Using the list of common types of information assets below, identify all types of consumer, employee and business information that your company handles. Mark the level of risk (Low, Medium, or High) for each item, or N/A if it is not applicable to your business. Use the following risk level descriptions as a guideline:

Level 1: Low Risk	Information you handle for customers, personnel, and your business that is publicly available.
Level 2: Medium Risk	This level of information generally includes information that is not Personally Identifiable Information (PII), or information that would not harm your customers, employees, or your business such as, phone numbers, office policies, vendor information, etc.
Level 3: High Risk	Highly sensitive information your business handles or has access to such as customer records, personnel files, credit/debit card numbers or other payment information, financial reports, passwords, PIN, social security numbers, etc. <i>Note: If this type of information is used by your company and is present on websites, computer systems, mobile devices or emails, it must be rated as Level 3: High Risk.</i>

Customer and Employee Information	Level of Risk
Individual addresses/phone numbers	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Email addresses	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Date of birth	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
SSN	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
Password/PIN	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
Photos/signatures	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
Account information	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Purchase/transaction history	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Criminal history	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Employee records	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
Medical records	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
Financial/banking	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
Legal documents	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Credit/debit card information	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
ACH/electronic payments	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
Paper checks	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
List other highly sensitive customer/employee information:	

Business Information	Level of Risk
Public information/brochures	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Press releases	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Social media postings	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Office policies	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Vendor information	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A

Management/board member credentials	<input type="checkbox"/> 1-Low	<input type="checkbox"/> 2-Medium	<input type="checkbox"/> 3-High	<input type="checkbox"/> N/A
Management/board reports	<input type="checkbox"/> 1-Low	<input type="checkbox"/> 2-Medium	<input type="checkbox"/> 3-High	<input type="checkbox"/> N/A
Email correspondence	<input type="checkbox"/> 1-Low	<input type="checkbox"/> 2-Medium	<input type="checkbox"/> 3-High	<input type="checkbox"/> N/A
Purchase orders	<input type="checkbox"/> 1-Low	<input type="checkbox"/> 2-Medium	<input type="checkbox"/> 3-High	<input type="checkbox"/> N/A
Accounting/financial	<input type="checkbox"/> 1-Low	<input type="checkbox"/> 2-Medium	<input type="checkbox"/> 3-High	<input type="checkbox"/> N/A
Marketing/sales	<input type="checkbox"/> 1-Low	<input type="checkbox"/> 2-Medium	<input type="checkbox"/> 3-High	<input type="checkbox"/> N/A
Legal/contracts	<input type="checkbox"/> 1-Low	<input type="checkbox"/> 2-Medium	<input type="checkbox"/> 3-High	<input type="checkbox"/> N/A
Medical/insurance records	<input type="checkbox"/> 1-Low	<input type="checkbox"/> 2-Medium	<input type="checkbox"/> 3-High	<input type="checkbox"/> N/A
Trade secrets/patents	<input type="checkbox"/> 1-Low	<input type="checkbox"/> 2-Medium	<input type="checkbox"/> 3-High	<input type="checkbox"/> N/A
List other highly confidential information that is the lifeblood of a company:				

Public-Facing Website	Level of Risk
<i>Identify and rate all information you collect and/or share with customers via a Website?</i>	
Personal information (names, address, phone, etc.)	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Account information	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Purchase/transaction history	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Accept online credit/debit card payments	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
Online enrollment or application forms	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
Financial information	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
Medical records	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input checked="" type="checkbox"/> 3-High <input type="checkbox"/> N/A
Legal documents	<input type="checkbox"/> 1-Low <input type="checkbox"/> 2-Medium <input type="checkbox"/> 3-High <input type="checkbox"/> N/A
List other sensitive information located on customer-facing Website(s)	

## VI. Network Security

*All of the sensitive information assets listed in the previous section must be protected.*

*This section will help to define your company's network security strengths and vulnerabilities, and assign a risk rating for the level of security provided.*

*If you use a third-party to manage networks, you may need to verify controls with them.*

Basic Network Controls	
Do you use firewalls, routers and other devices to protect your network?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are firewalls, routers, and other devices securely configured to control access?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Have the following configuration steps been completed?	
Changed the default admin passwords	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Removed unneeded services	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

Do you use updated anti-virus and anti-spyware software:	
On all desktop computers with automatic update	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
On all computers and servers with automatic update	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
To Scan all incoming email	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do you regularly update software and security patches:	
On all desktop computers with automatic update, where available	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
On all computers and servers with automatic update, where available	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

<b>Secure Access to Information: Network Servers</b>	
How do you limit access to your network? (Check all that apply)	
<input type="checkbox"/> No controls, or use shared log on	
<input type="checkbox"/> Unique user ID and password	
<input type="checkbox"/> Unique user ID, password, plus additional authentication is required	
Do you use employee permission controls to restrict access to authorized users?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Is employee access to the network monitored?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Are unsuccessful log on attempts monitored?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Is email used to send or receive sensitive information?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
If so, is the email encrypted?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

<b>Secure Access to Information: Wireless and Remote Access</b>	
Do you allow remote access to your network?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
If Yes, how do you secure your remote access? (Check all that apply)	
<input type="checkbox"/> Unique user ID and password <input type="checkbox"/> VPN or similar <input type="checkbox"/> VPN with additional authentication required	
Do you require minimum security standards (anti-virus, firewall, etc) for computers with remote access?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do you have a wireless network?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
If Yes, is the wireless network secured? (Note, WEP is not a secure encryption protocol for wireless networks.)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Is the wireless network for "guest" access and is it on a separate subnet from the rest of the network?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

<b>Secure Access to Information: Public-Facing Website</b>	
Do you have sensitive customer information on your Website? (If no, skip this section)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Is your public-facing Website hosted by a third party vendor?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
If yes, are third party vendor contracts up-to-date and cover all expectations for security?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
How is your public-facing Website(s) secured? (Check all that apply)	
<input type="checkbox"/> Unique user ID and password	
<input type="checkbox"/> Additional authentication is required	
<input type="checkbox"/> Firewall	
<input type="checkbox"/> Encrypted with Secure Socket Layer (SSL)	
<input type="checkbox"/> Other	

Secure Access to Information: Payment Card Handling	
Do you accept credit cards and other payments from your Website? (If no, skip this section)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
If yes, Is the payment process PCI certified?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do you use a third party vendor(s) to process credit cards and other payments from customers?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
If yes, are third party vendor contracts up-to-date and cover all of expectations for security?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
If yes, does your business follow PCI, SSAE 16, SAS70, HIPAA or other guidelines for "controlling employee access" to this information?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

Storage of sensitive information		
Do you store sensitive information on any of the following media? If Yes, is it encrypted?	Sensitive Data	Encrypted
Network files/database	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Desktop computers	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Laptops/tablets	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Mobile phones/devices	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Flash drives, CD, DVD, or other portable storage	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Backup tapes and other media	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Cloud data storage	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Other: _____	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No

Disposal of Information	
Do you remove unnecessary files or data at least annually, especially sensitive information?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
How is sensitive information permanently destroyed? (Check all that apply)	
<input type="checkbox"/> Electronic files and data are securely removed	
<input type="checkbox"/> Paper checks and records with sensitive data is cross-shredded	
<input type="checkbox"/> Third party vendor is used to shred documents or remove data	
<input type="checkbox"/> Data is permanently removed before equipment is sold or discarded	
Are there regular audit reviews of the company's disposal policies?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

Data Breach Loss/Back up/Disaster Recovery	
Do you have alternative (redundant) hosting facilities in the event of failure?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Do you have an acceptable procedure for back up of your data?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Where is your back up data stored? (Check all that apply)	
<input type="checkbox"/> On a redundant storage device on site	
<input type="checkbox"/> Backup media is moved to a secure off-site storage location	
<input type="checkbox"/> Online backup provider	
Is the backup information encrypted? (Check all that apply)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
<input type="checkbox"/> The backup media is encrypted (tapes, hard drives, etc.)	
<input type="checkbox"/> Online backups use a secure connection (e.g. SSL)	
<input type="checkbox"/> Backups are encrypted at rest (e.g. redundant storage device or online backups are encrypted on the server)	

Intrusion Systems	
Is there an intrusion detection or prevention system used in the company's network?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
Is a vulnerability scan or penetration test performed on all Internet-facing systems?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
List other network security issues for your business:	

Rate your Network Security risk on a scale of 1-5, with 1 being the least secure, and 5 the most secure:					
Least Secure	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4 <input type="checkbox"/> 5	Most Secure
Reason for the rating:					
List areas of high risk (threats):			List new controls needed:		